FINANCIAL INTELLIGENCE ANALYSIS UNIT

MALTA GAMING AUTHORITY

CONSULTATION DOCUMENT

APPLICATION OF ANTI-MONEY LAUNDERING AND COUNTERING THE FUNDING OF TERRORISM OBLIGATIONS TO THE REMOTE GAMING SECTOR

Issued: 10 July 2017
Closing Date: 11 August 2017

1. Introduction

This document is a joint publication of the Financial Intelligence Analysis Unit ("FIAU") and of the Malta Gaming Authority ("MGA") on the forthcoming application of anti-money laundering and combatting the funding of terrorism ("AML/CFT") requirements to holders of licences to operate games of chance and games of chance and skill via means of distance communication ("licensees"). These obligations will enter into force by virtue of the transposition into Maltese law of Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing ("the Directive").

The purpose of this document is to provide a general explanation of the main AML/CFT obligations and a general outline of how licensees will be expected to comply with these obligations. This document will serve as the basis for a more detailed sector-specific guidance document that will be issued at a later stage following due consultation with the remote gaming sector.

The document is divided into five main sections, each of which corresponds to what is considered by the FIAU and the MGA ("the Authorities") as being the main AML/CFT obligations of subject persons. This document does not cover all AML/CFT obligations and the omission of any reference to other AML/CFT obligations is not to be considered as tantamount to the inapplicability of the same. Moreover, this document does not set out how the Authorities are to exercise the discretion allowed to Member States under art 2(2) of the Directive.

Licensees are strongly encouraged to read this document in conjunction with the Directive as well as with Part I of the current Implementing Procedures. While the transposition will inevitably result in changes to the Implementing Procedures, the general content thereof is unlikely to undergo any major change.

It is important for Licensees and other interested parties to note that the current document consists only of proposals. Accordingly, the Authorities are not bound by the contents of the present document which are subject to changes and revisions following any feedback received from Licensees and other interested parties.

Licensees and other interested parties are invited to submit any feedback they may have in relation to this document on the email address provided hereunder. This document, together with the feedback received, will form the basis of the sector-specific guidance to be issued by the Authorities. Submissions may be made on legal@fiumalta.org until the 11 August 2017.

2. The Risk-Based Approach

2.1 What is the Risk-Based Approach?

Licensees may already be aware that the AML/CFT regulatory framework that will be applicable to them as subject persons adopts a risk-based approach, i.e. it requires subject persons to adopt measures, policies, controls and procedures that are commensurate to the money laundering and funding of terrorism ("ML/FT") risks to which they are exposed to prevent and mitigate the said risks from materialising themselves. The risk-based approach recognises that the ML/FT risks faced by each sector and each subject person are different, and allows for resources to be invested and applied where they are most required. It is diametrically opposed to a prescriptive tick-box approach and entrusts subject persons with significant discretion in its application.

2.1.1 The Risk Assessment

The cornerstone of the risk-based approach is the risk assessment which has to be carried out at different stages of a subject person's activities. This assessment allows the subject person to identify its ML/FT vulnerabilities and the ML/FT risks it is exposed to. On this basis, the subject person will be able to draw up, adopt and implement AML/CFT measures, policies, controls and procedures that address any identified risks.

However, each customer exposes the subject person to different risks. A customer-specific risk assessment must therefore be carried out so that the subject person is able to identify potential risks upon entering into a business relationship with or carrying out an occasional transaction for a customer. This assessment enables the subject person to develop a risk profile for the customer and to categorise the ML/FT risk posed by such customer as low, medium or high.

Subject persons must subsequently ensure that the AML/CFT measures, policies, controls and procedures adopted are sufficiently flexible to allow a subject person to address the specific ML/FT risks arising from the particular business relationship or occasional transaction. How these measures, policies, controls and procedures are to be applied to particular risk scenarios has to result from the subject person's Customer Acceptance Policy.

2.1.2 The Risk Areas

The risk areas that the business risk assessment as well as the customer-specific risk assessment are to look at can be divided into four, i.e. customer risk, product/service/transaction risk, interface risk and geographical risk. The form they may take within the remote gaming sector is explained in further detail in Section 2.2.2 hereunder.

2.1.3 The Risk Assessment as a Dynamic Tool

An effective risk assessment has to be a dynamic one. Subject persons have to ensure that they revise the same when there are significant developments within the environment within which they are operating and within their business structures/activities. Any such changes can lead the subject person to be exposed to new ML/FT risks. Identifying the same through a revision of the risk assessment allows the subject person to take action to ensure that its measures, policies, controls and procedures are robust enough to cater for these. It is therefore important that subject persons always

take into consideration any supranational, national or sectoral risk assessment that may be available when conducting and revising their own specific risk assessment.

Even the customer-specific risk assessment has to be revised when the business relationship entertained with the customer undergoes changes. Once the customer has begun his planned operations or has begun transacting through an account, depending on the type of business it is important that the subject person monitors this activity to ensure that it is in line with the customer's profile. Any changes in the customer's pattern of activity must be analysed to determine whether an update of the customer's profile is necessary.

2.1.4 Unchanging High Risk Situations

It is important to note that independently of the risk assessment carried out by the subject person, there will always be instances that are deemed to be high risk. One such instance is dealing with Politically Exposed Persons ("PEPs"), their family members or close business associates ("persons linked thereto"). In such cases, the regulatory framework itself sets out the measures to be applied to adequately address the risks arising from dealing with the said individuals. This aspect is considered further in Section 3.2.1.

2.2 Proposed Application to the Remote Gaming Sector

2.2.1 The Business and Customer-Based Risk Assessments[1]

The Authorities are not at present considering applying any derogation from the requirement to carry out business specific risk assessments for the gaming sector, which is possible in terms of article 8(2) of the Directive. Licensees will therefore be required to carry out a business risk assessment to identify the ML/FT risks they are exposed to and ensure that the measures, policies, controls and procedures adopted are sufficiently robust to prevent and mitigate the same. The business risk assessment has to be documented and approved by the Board of Directors (or equivalent) of the licensee, and made available to the Authorities upon request.

The MGA has completed a sectoral ML/FT risk assessment which enabled it to identify some risk factors that licensees are to take into account when drawing up their business risk assessment. Risk factors within the remote gaming context are considered further in Section 2.2.2. hereunder. Licensees should also take into consideration and factor in their business risk assessments the outcomes and recommendations of Supra-National and National Risk Assessments that may be issued from time to time.

Licensees will be expected to revise their business risk assessment whenever there are changes to the environment within which they are operating and within their business structures/activities. Thus, situations such as a widening of the customer-base or the addition of games and payment methods

[1] *For a better understanding of subject persons' obligations relative to the conduct of risk assessments, licensees are invited to consult article 6 to article 8 of the Directive. Chapter 4 of Part I of the current Implementing Procedures also provides a description of what is the risk-based approach. However, licensees are to note that this Chapter is to be revised by the FIAU as part of the transposition of the Directive into Maltese law. Additional insights into the risk-based approach can be derived from the FATF Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing - High Level Principles and Procedures.*

which present a different risk profile from those already offered should lead to a revision of the business risk assessment. The same applies when the licensee changes its structure or undertakes major operational changes. In the absence of any of the above, licensees should assess their business risk assessment at least once a year, to evaluate whether any changes thereto are necessary.

Licensees may engage external consultants to assist them in the drawing up and the revision of their business risk assessments. However, it will be necessary for any report, findings and conclusions to be adopted by the licensee who retains responsibility to ensure it complies with its obligation to carry out a business risk assessment.

As regards the customer specific risk assessment, it is being proposed that in all circumstances this be carried out at the inception of the business relationship or prior to the carrying out of an occasional transaction. In view of the proposal put forth in Section 3.2.1 of this Document, it is very likely that this initial customer specific risk assessment will have to be revised at some point after the establishment of the business relationship and this may result in a customer's risk rating having to be similarly adjusted.

2.2.2 Risk Factors Specific to the Remote Gaming Sector

i. Customer Risk – The risk of ML/FT may vary in accordance with the type of customer. The assessment of the risk posed by a natural person is generally based on the person's economic activity and/or source of wealth. A customer having a single source of regular income will pose a lesser risk of ML/FT than a customer who has multiple sources of income or irregular income streams.

ii. Product/Service/Transaction Risk – Some products/services/transactions are inherently more risky than others and are therefore more attractive to criminals. These include products/services/transactions which are identified as being more vulnerable to criminal exploitation such as gaming products or services that allow the customer to influence the outcome of a game, be it on his own or in collusion with others. The use by customers and the acceptance by licensees of specific funding methods should also be treated as high risk factors. This includes cash and other payment method that may not leave or disrupt the audit trail and allow the customer to operate with a degree of or complete anonymity such as pre-paid cards or virtual currencies. The exceptional use by a customer of accounts held or cards issued in the name of third parties is also to be regarded as a high risk factor. Conversely, where a customer transfers funds from a bank account or a card linked to a bank account held in his name with an institution established in a reputable jurisdiction, the risk of ML decreases – these credit or financial institutions are themselves subject persons and one would expect that as part of their CDD obligations they would monitor on an on-going basis any account or card activity.

   The sector-specific risk assessment has allowed the MGA to obtain an indication of the risks associated with various products/services/transactions, which indicators have been included in Appendix I to this document, to assist licensees in the conduct of their business risk assessment and the evaluation of the product/service/transaction risk they are exposed to.

iii. Interface Risk – The channels through which a licensee establishes a business relationship and/or through which transactions are carried out may also have a bearing on the risk profile

of a business relationship or a transaction. Channels that favour anonymity increase the risk of ML/FT if no measures are taken to address the same. However, licensees may want to note that situations where interaction with the customer takes place on a non-face to face basis will no longer be considered as automatically high risk as long as technological measures are in place to address the heightened risk of identity fraud or impersonation present in these situations.

It is the Authorities' opinion that the use of technological measures outlined in Section 3.1.1.2 (b) of Part I of the current Implementing Procedures under numbers (2) to (4) are sufficiently effective to counter the above mentioned risks emanating from the fact that the potential customer is not sighted physically prior to the provision of gaming services. These measures allow a licensee to establish whether or not the customer providing the relative identification details is actually the person he alleged to be.

On the other hand, the use of electronic databases as provided for under Section 3.1.1.2 (b) of Part I of the current Implementing Procedures under number (1) only allows for determining whether the identification details provided correspond to those of an actual person but does not provide sufficient comfort in establishing whether the customer is that individual. Hence, the risk inherent in non-face to face transactions will not have been sufficiently addressed and additional risk mitigation measures in the form of enhanced due diligence would become necessary.

Licensees are furthermore invited to bring to the attention of the FIAU any additional technological measures they consider as equivalent to those referred to in Section 3.1.1.2 (b) of Part I of the current Implementing Procedures for the FIAU's consideration.

The interface risk also increases where the customer does not interact directly with the licensee but there is present a third party who involves itself in the placing of wagers on behalf of the customer and/or the withdrawal of winnings. This is especially the case where these third parties are not themselves subject to any form of AML/CFT obligations. The use of physical establishments by a licensee to extend its network and provide gaming services to customers on its own behalf (i.e. the licensee's) is not considered to be an outright high-risk indicator, subject to certain pre-requisites as set out in Section 3.1.2(i) being met.

iv. Geographical Risk – The geographical risk is the risk posed to the licensee by the geographical location of the business/economic activity and the source of wealth/funds of the business relationship. The nationality, residence and place of birth of a customer should also be taken into account as these might be indicative of a heightened geographical risk. Countries that have a weak AML/CFT system, countries known to suffer from a significant level of corruption, countries subject to international sanctions in connection with terrorism or the proliferation of weapons of mass destruction as well as countries which are known to have terrorist organisations operating within are to be considered as high risk. The opposite is also true and may therefore be considered as presenting a medium or low risk of ML/FT.

3. CUSTOMER DUE DILIGENCE

3.1 What is Customer Due Diligence?

The determination of a customer's risk profile is essential to allow a subject person to apply a level of Customer Due Diligence ("CDD") commensurate to the identified ML/FT risk. CDD is intended to allow the subject person to know who its customer is and to build a customer profile on the basis of which the subject person would be able to assess the customer's activity to identify any unusual behaviour. Any such behaviour has to be questioned and, if it is found to lead to a suspicion of ML/FT, it also needs to be reported to the FIAU. The documentation and information collected will then assist the authorities in any analysis or investigation of the suspected instance of ML/FT.

3.1.1 The CDD Measures

CDD consists of four measures:

i. Identification, which consists in the collection of a series of personal details which at present consist of the individual's full name, residential address, place and date of birth, nationality and, to the extent applicable, an identity reference number. Identification has to be carried out with respect to the customer and, where applicable, the beneficial owner. The customer is the person with whom the subject person enters into a business relationship or on whose behalf it carries out a transaction. The beneficial owner, where applicable, is the individual who ultimately owns and controls the customer. In situations where the person who approaches a subject person for a service/product is acting on behalf of someone else, the subject person would need to also identify the agent and ascertain itself that it is authorised to act on the customer's behalf.

ii. Verification of the identity of the agent, the customer and the beneficial owner, as may be applicable, which is to be carried out by checking that the personal details provided by the person match with those reported by independent and reliable sources. For the purposes of this obligation, a reliable and independent source includes, *inter alia*, a government authority, department or agency, a regulated utility company or a subject person carrying out relevant financial business in Malta, in a Member State of the EU or in a reputable jurisdiction, since these entities would have already checked the existence and characteristics of the persons concerned.

iii. Obtaining information on the purpose and intended nature of the business relationship.

iv. Conducting ongoing monitoring of the business relationship including:

    a. The scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the subject person's knowledge of the customer, the business and risk profile, including where necessary the source of funds.

       The proper scrutiny of transactions requires that the subject person acquires information on the customer's source of wealth. Source of wealth consists in determining how the customer acquired his net worth and whether the same justifies the service/product

requested and the use being made thereof: it is not and should not be considered as a forensic exercise. On the basis of this information licensees will be able to identify unusual behaviour or transactions and to question the same. As to the extent of the information that licensees are to collect, this depends very much on the risk profile of the customer. Where the risk is medium or lower, a declaration from the customer with some details (e.g. nature of employment/business, employer etc.) would suffice. However, where the risk of ML/FT is higher and where the customer's activities are dubious or do not fit within his profile any such declaration would need to be supplemented by more specific information and documentation.

Unlike source of wealth, source of funds relates to how the funds used for a particular transaction were obtained by the customer. As long as a transaction falls within the profile of the customer, there is no need for subject persons to obtain specific information and documentation on the same; it is only where a transaction presents a departure from the known behaviour of a customer that a subject person is required to question the same and obtain sufficient information and documentation on the matter. It is also one of the situations in which the risk profile of the customer may have to be revised.

b. Ensuring that the documents, data or information held are kept up-to-date.

The level of on-going monitoring will inevitably depend on the risk profile of the customer but even in low risk situations there must be a degree of oversight taking place.

These measures are to be applied whenever a subject person carries out an occasional transaction or otherwise enters into a business relationship. However, it is to be noted that only in the case of a business relationship that a subject person has to apply all four CDD measures. Where the subject person is carrying out an occasional transaction, the subject person has merely to apply the initial two measures and, in high risk scenarios, it is also recommended that it identifies what is the source of funds. An occasional transaction is a transaction other than a transaction carried out within a business relationship. In determinate sectors the application of CDD measures in the case of occasional transactions depends on the value thereof.

3.1.2 Proposed Interpretation of CDD requirements for the Remote Gaming Sector

i. Business Relationships and Occasional Transactions

A licensee will be considered as a subject person whenever it is providing services to a customer so that he may wage a stake with monetary value in a game of chance, including those with an element of skill. It is the Authorities' understanding that licensees entertain business with customers who are predominantly individuals and who act in their own name and on their own behalf. It is also the Authorities' understanding that licensees open accounts for all, or at least the majority of, their customers, which is indicative of a relationship that is expected to have or has an element of duration and therefore of a business relationship. Subject to what is stated further on in Section 3.2.1, it is expected that licensees will be required to apply all four CDD measures. This entails that the licensees will not only have to identify their customers but also verify their identity, assess and where appropriate, obtain information on the purpose and intended nature of the relationship and carry out on-going monitoring in line with the customer's risk profile.

In the event that the licensees carry out occasional transactions, the obligation to carry out CDD will be dependent on the value of the said transaction reaching or exceeding Euro two thousand (€2000). Licensees would find themselves subject to the said obligation also in the case where they execute a series of linked transactions which, though individually below the Euro two thousand (€2000) threshold, when taken cumulatively meet or exceed the said threshold. Transactions are considered as linked if for example they are carried out by the same customer through the same game or in one gaming session. In this context, the licensee would have to identify the customer, verify his identification and, if deemed high risk, establish the source of funds used in the occasional transaction. These measures would have to take place either upon the wagering of stakes or the collection of winnings. It is to be remarked that carrying out CDD at the earliest possible may limit situations in which a licensee receives tainted funds and subsequently finds it hard to dispose thereof.

The occasional transaction scenario may be relevant to licensees if they make use of physical establishments to extend their customer reach. Where the customer only makes use of the terminals present within the physical establishment so as to open an account in his own name with the licensee or to use such an account, the interaction between the two would still be considered to be a business relationship subject to the requirements envisaged in this section.

On the other hand, if the customer makes use of an account held by the operator of the physical establishment to carry out occasional transactions with the licensee, the licensee has to ensure that the AML/CFT policies and procedures applied by the physical establishment allow for the identification and verification of the customer once the relative threshold is reached, as set out hereabove. Where these physical establishments are located in a jurisdiction other than Malta but are (i) subject to authorisation and supervision; and (ii) have to meet AML/CFT obligations equivalent to those envisaged under the Directive, the licensee may consider that it is meeting its own AML/CFT obligations under Maltese law if it ascertains itself that the operator of any such physical establishment is effectively complying with AML/CFT obligations equivalent to those envisaged under the Directive as applicable in that other jurisdiction. Hence, the licensee is expected to:

a. Identify of the operator of the physical establishment (and verify the same) and ensure that there are no obstacles to the effective implementation of AML/CFT requirements by the said operator;

b. Be provided with the details of any customers identified by the operator of the physical establishment;

c. Scrutinise the activity taking place through the physical establishment's account and ensure that the operator of the physical establishment does not adopt practices which allow it to circumvent its AML/CFT obligations.

ii. Identification and Syndicate Relationships

In applying the CDD measures set out in Section 3.1.1, licensees are to especially note that:

a. Personal Details - The Authorities are aware that gaming legislation already requires licensees to obtain a number of personal details on a prospective customer, these being

the official full name, the date of birth and permanent residential address of the individual. However, it should be noted that at present under Part I of the Implementing Procedures, identifying an individual involves obtaining these personal details as well as the individual's place of birth, nationality and, to the extent applicable, an identity reference number.

The additional personal details that subject persons are required to collect in terms of Section 3.1.1.2 (i) of Part I of the Implementing Procedures are especially intended to allow the subject person to have a better understanding of the actual ML/FT risk. An individual's nationality and place of birth are factors that connect the person concerned with one or more jurisdictions, providing the subject person with basic information to allow it to determine what is the geographical risk presented by the particular business relationship or occasional transaction.

While the Implementing Procedures will have to be revised as part of the Directive's transposition into national law, the concept of identification is not expected to undergo particular changes and licensees will be expected to identify customers as currently defined in the Implementing Procedures Part I.

b. Syndicates – The Authorities are aware that at times licensees provide their services and products to syndicates funding one or more players. In such circumstances, where the funds being wagered by are collected from multiple persons who will share in any winnings, the particular transaction will not only be considered as having been undertaken on behalf of the customer but also on behalf of those other persons providing the necessary funding. The persons are to be considered as beneficial owners and licensees are therefore required to identify and verify their identity.

3.2 Extent and Timing of CDD

The initial three elements of CDD are carried out at the inception of the business relationship or when the occasional transaction is to take place. However, the application of the risk-based approach allows subject persons to vary the extent and timing of CDD measures carried out depending on whether the particular business relationship or occasional transaction is rated as presenting a high, medium or low level of ML/FT risk. This allows for:

i. The carrying out of Simplified CDD ("SDD") in low risk situations, i.e. for identification and a sufficient level of on-going monitoring to be carried out but with verification and obtaining additional information on the business relationship postponed until a particular event takes place or a pre-established threshold is reached. However, it would still be necessary to determine whether the customer is a PEP or related to one. It is important to note that in situations where it may be possible to apply SDD but the subject person suspects ML/FT, the subject person is precluded from applying SDD.

ii. The carrying out of Enhanced CDD ("EDD") in high risk situations, i.e. taking more stringent steps in the application of CDD with special regard to the information to be collected on the purpose and intended nature of the business relationship and on-going monitoring. In particular, obliged entities would be expected to not only obtain information on the source of wealth and the source of funds but to substantiate the same with adequate documentation.

In some cases the measures to be applied are set out by law as is the case of PEPs and persons associated therewith.

In all those other situations where the risk is neither low as to allow the application of SDD nor high to warrant the application of EDD, a subject person is expected to apply all four CDD measures, the initial three of which have to be complied with when establishing the business relationship.

Where the subject person is unable to fulfil its CDD requirements at customer on-boarding stage (i.e. identification, verification and determining the purpose and intended nature of the business relationship) because of the customer's own reluctance, the subject person is precluded from establishing the business relationship or carrying out of the occasional transaction. Moreover in such cases the subject person has to consider whether there are reasonable grounds to suspect ML/FT which would necessitate the submission of a suspicious transaction report with the FIAU and, having ascertained that there are no restrictions[2], return any funds in its possession to the originator thereof through the same channels.

3.2.1 Proposed Application of CDD Requirements - Low Value Activity

The Directive states that CDD has to be carried out whenever a business relationship is established or an occasional transaction takes place. Specifically to the gaming sector, an occasional transaction is equated with the collection of winnings, the wagering of stakes or both of Euro two thousand (€2000) or more. Thus, no CDD needs to be carried out by a licensee in the case of an occasional transaction unless the said threshold is met or exceeded. On the other hand, in the case of a business relationship licensees will be required to carry out CDD upon the establishment of such a relationship.

However, it is the Authorities' understanding that at the inception of a business relationship in most cases the funds deposited by a customer will involve a minimal amount. Moreover, the Authorities also understand that the nature of the product/service offered by licensees usually requires a quasi-instant execution and therefore delaying the establishment of the business relationship for the purpose of carrying out particular CDD requirements in such scenarios could significantly affect the ordinary conduct of business.

Given these circumstances and in the absence of any high risk factors, the Authorities consider that there are therefore the grounds to consider such business relationships as posing a lower risk of ML/FT and apply SDD. This entails that only identification and a sufficient level of on-going monitoring would have to be carried out when establishing the business relationship, with the other CDD measures to be applied once a determinate threshold or a particular stage in the particular relationship is reached.

In the context of remote gaming operators, the Authorities are therefore proposing the following approach:

i. When approached to open an account, the licensee is to carry out a customer risk assessment. To the extent that it does not result from the customer risk assessment to

[2] The obligation to ascertain whether there are any restrictions on the release of funds back to the originator entails that a subject person has to ascertain whether an order or notice has been issued in terms of the Prevention of Money Laundering Act, the Criminal Code or the Prevention of Money Laundering and Funding of Terrorism Act prohibiting *inter alia* the transfer of funds to the person concerned.

be carried out that the business relationship presents a high risk of ML/FT, or that the customer is a PEP or linked to one, the business relationship can be deemed a low risk one and the licensee will be able to apply SDD. Thus, in these circumstances the licensee may limit itself to carrying out identification and a level of on-going monitoring and delay carrying out the other CDD measures up until certain events happen or thresholds are met as set out in (ii) hereunder. Thus, it will not be necessary to verify the customer's identity nor to collect information on the source of wealth at the outset of the relationship.

Within this context, on-going monitoring would be limited to ensuring that the transactions carried out do not exceed the threshold set out in (ii) hereunder; if the threshold is exceeded, the subject person will have to carry out the CDD measures still pending. Thus, it is important that licensees have measures in place to ensure that the triggering of the threshold is not circumvented through the opening of accounts under fictitious names. Given the limited nature of on-going monitoring, there will be no need for the licensee to collect any information on the customer's source of wealth until such time as the thresholds set out in (ii) hereunder are met.

Licensees should always remember that:

a. They cannot apply SDD if the risk assessment reveals that the business relationship is exposing them to a high risk of ML/FT in which case they are expected to apply EDD measures, i.e. not only would they not be able to delay the carrying out of CDD measures but they would have to intensify the same as described in Section 3.2.2 hereunder;

b. In situations where the only high risk factor is the presence of a PEP or a person linked thereto, they would have to also apply EDD measures as explained in (iv) hereunder; and

c. They are precluded from applying SDD when they suspect ML/FT.

ii. Where SDD has been applied at the inception of the business relationship, the licensee will have to carry out verification and collect any other information necessary to build a better profile of the customer, including source of wealth, when the customer effects deposits in the gaming account amounting to Euro two thousand (€2000) or more, whether in a single transaction or a series of transactions adding up to the said amount. To the extent that a licensee can distinguish between deposits made by the customer from own funds and funds received from other sources such as bonuses given by the licensee itself, the Euro two thousand threshold is to be calculated only on the basis of deposits from own funds. No activity is to be allowed on the customer's account until such time as CDD is completed.

In applying CDD or EDD, it will be especially important for licensees to establish the customer's source of wealth. Licensees may do so by obtaining information from the customer himself (e.g. nature of employment and employee details, type of business involved in etc.). Licensees are not required to obtain supporting documentation in all instances but should do so when they do not consider the information provided by the customer to be satisfactory or reliable and also in higher risk relationships.

iii. Notwithstanding what is provided in (i) above, where the only element of high risk is the funding method used by the customer, the licensee may still apply SDD but the requirement to carry out verification and collect any other information necessary to build a better profile of the customer, including source of wealth, will be triggered when the customer effect deposits in the gaming account Euro one hundred and fifty (€150) or more, whether in a single transaction or a series of transactions adding up to the said amount. To the extent that a licensee can distinguish between deposits made by the customer from own funds and funds received from other sources, the Euro one hundred and fifty threshold is to be calculated only on the basis of deposits from own funds. It is therefore important that licensees have measures in place to ensure that the triggering of the threshold is not circumvented through the opening of accounts under fictitious names. No activity is to be allowed on the customer's account until such time as CDD is completed.

iv. Licensees are expected to take the necessary action to identify PEPs and associated persons upon the establishment of a business relationship or prior to the carrying out of an occasional transaction in all cases even in lower risk scenarios. In low risk scenarios as described above this can be done by obtaining a declaration from the customer as to whether he is a PEP or not. In the event of a customer declaring that he is a PEP, the licensee can only proceed with establishing the business relationship or carrying out the occasional transaction only after obtaining approval by the licensee's senior management. Where a customer declares that he is a PEP, the licensee should also demand him to disclose the position/office he occupies or function he carries out. As part of the on-going monitoring, the licensee is also expected to screen customers against reliable PEP databases so as to ascertain itself that its records are up-to-date.

It is felt that this approach will allow licensees the necessary flexibility to meet their AML/CFT requirements without unnecessarily disrupting their operations. The Authorities do acknowledge that this approach may lead to a greater incidence of situations in which licensees will be in possession of funds belonging to customers in relation to whom they had to end the business relationship due to incomplete CDD. In this case, once the licensees have ascertained that there is no restriction on the transfer or release of the funds, licensees should transfer the funds to source using the same channels through which they received them and consider whether there are grounds to file a STR.

Given the different funding methods that may be used in the remote gaming sector, the Authorities are also conscious that licensees may find it impossible to remit the funds back to the customer through the same channels. In such exceptional circumstances and as a measure of last resort, licensees should remit the funds to a bank account held with a credit institution in a reputable jurisdiction in the customer's name. When remitting funds in these circumstances, licensees are to indicate in the script/instructions accompanying the funds that these are being remitted due to their inability to complete CDD.

It is important to note that low value activity is only one instance in which SDD can be applied. It is not excluded that there may be other situations in which licensees may deem the risk of ML/FT to be low therefore allowing the licensee concerned to apply SDD.

3.2.2 Proposed Application of CDD in the course of a Business Relationship

Once the conditions referred to in Section 3.2.1 (ii) above are met, licensees are expected to carry out the remaining CDD measures, i.e. verification of identity, establish the nature and purpose of the business relationship, obtain information on the source of wealth, and revisit the risk assessment of the customer. From the customer risk assessment, the licensee may conclude that the particular business relationship presents a low, medium or high risk of ML/FT. This will influence the level of CDD to be carried out as well as the level of on-going monitoring to which transactions carried out within the context of a given business relationship will be subject to.

Where from the risk assessment the licensee concludes that the customer presents a low, medium or high level of ML/FT risk, the licensee will have to carry out SDD, CDD or EDD accordingly. In all cases, the licensee will have to carry out the same measures in so far as verification of identity and understanding the nature and purpose of the business relationship is concerned, and gathering information on the source of wealth. In fulfilling this last requirement, licensees should obtain sufficient information even from the customer himself in relation to the activities through which he generates his wealth and which will allow him to fund transactions carried out in the course of the business relationship. At this point it will be sufficient if the licensee obtains detailed information on the source of wealth from the customer himself (e.g. employed with X Ltd as an accountant). Having a rough estimate of what may be the expected volume and quantity of transactions passing through the account would also help the licensee as this information together with the source of wealth will be a major aid in conducting on-going monitoring.

Where the risk assessment leads the licensee to consider a customer as high risk, the licensee is required to apply EDD measures. The nature of the measures applied will depend on the high risk factors identified. To the extent that the risk factor is a result of the non-face to face nature of the relationship and the absence of any technological measure, the EDD measures applicable in the case of verification of identity can take the form of one of the EDD measures currently set out in the Implementing Procedures Part I (Section 3.5.1). More important still will be the information and documentation that will need to be collected when it comes to source of wealth as a high risk situation will inevitably demand that a licensee enhances its understanding of the activities generating the wealth of a customer. In such circumstances licensees will have to obtain more specific information and supporting documentation (e.g. it will not be sufficient for the licensee to be told that the source of wealth is the result of the customer's income derived from his employment with X but it will be necessary for the licensee to obtain copies of the employment contract, statements of earnings etc.). This is especially important where there is a PEP or person linked thereto as delving deeper into the source of wealth is one of the EDD measures statutorily provided for. The extent of the information and documentation to be collected cannot be pre-set but has to be appreciated on a case-by-case basis and until the licensee can be said to have any questions answered or doubts dispelled.

As already stated in Section 3.2.1 above, it is still possible that a business relationship will present a low risk of ML/FT even though the activity on the customer's account can no longer be considered as low value. Should this be the case, licensees are still entitled to apply SDD though it will no longer be possible to delay verification of the customer's identity and the collection of information, such as his source of wealth, to build the customer's profile. However, licensees will be able to vary the extent of the verification to be carried out and of the information to be collected to create a complete customer profile.

The level of risk identified will also determine the level of on-going monitoring conducted. Independently of whether a relationship was considered as posing a low, medium or high risk, a minimal level of on-going monitoring will always be required consisting in ensuring that (a) the CDD documentation collected is kept up-to-date at all times; and (b) the circumstances leading to the specific risk categorisation do not undergo any change. Where changes to the elements in the business relationship are noted, the licensee has to examine whether these changes impact the allocated risk level and take any necessary corrective measures.

In situations where the risk present is medium or high, transactions need to also be screened to ensure that they are in line with the risk profile of the customer and especially that the transactions reflect the source of wealth of the customer. In situations where the licensee notices discrepancies or unusual transactions, the licensee has to understand the reason behind these discrepancies or transactions and take any action necessary. This may include collecting information and documentation as may be applicable on the source of funds, i.e. from where the funds used in a particular transaction were derived. In high risk situations, licensees would be expected to also collect supporting documentation and not merely rely on any customer declarations.

3.2.3 Proposed Application of CDD Requirements Licensees' Existing Customers

The Authorities are aware that licensees already have a number of business relationships in relation to which they will have to apply the CDD measures described above upon the transposition of the Directive into Maltese legislation. The Authorities also acknowledge that this is not an exercise which can be carried out at once and it is therefore proposing that this be carried out on the following basis:

i. Licensees are to identify those business relationships in relation to which the Euro two thousand (€2000) threshold determined on the basis of the criteria set out in 3.2.1 above has already been met or exceeded and those in relation to which the said threshold has still to be reached. This has to be determined on the date when licensees become subject to AML/CFT requirements.

ii. In relation to those business relationships where it is determined that the Euro two thousand (€2000) threshold has yet to be met, the licensee would have to ensure that it collects the additional information to meet the SDD requirements set out in Section 3.2.1 above. On the other hand, where the Euro two thousand (€2000) has already been reached or exceeded, the licensee would have to adopt the required level of CDD as set out in 3.2.2 above.

iii. Licensees are to carry out this exercise on a risk-sensitive basis. Thus, the higher the risk of ML/FT to which a licensee is exposed through an existing business relationship, the sooner a licensee is expected to adopt the necessary CDD measures. In determining risk, licensees are expected to consider the information they already have at their disposal, the length of time the business relationship has been established, the volume of transactions carried out and the size of wagers etc.

iv. While this exercise is risk-driven, the Authorities expect that the review of existing business relationships be completed within a reasonable period of time. Business relationships deemed high risk are to be revised within six (6) months from when licensees become subject to AML/CFT obligations. All other business relationships should be

reviewed within eighteen (18) months of the licensee becoming subject to AML/CFT obligations. Notwithstanding these time limits, the review is to be completed within the shortest time period possible.

v. To collect the necessary information and, to the extent applicable, documentation, licensees may adopt any system they consider as workable given the frequency of transactions carried out. In situations where an account is used frequently, the licensee may wish to solicit any information or documentation when the customer tries to make use of the account. On the other hand, for inactive accounts licensees may request the same through mail shots.

4. RELIANCE, AGENTS AND OUTSOURCING[3]

The AML/CFT regulatory framework does allow for the exercise of reliance, with the subject person relying on the information and documentation collected at customer on-boarding stage by any other person in an EU Member State or a reputable jurisdiction who is subject to AML/CFT requirements and supervision equivalent to those required in terms of the Directive. In determining as much, a subject person can refer to FATF/Moneyval evaluation reports, IMF Country Reports etc.

When exercising reliance, a subject person can obtain the identification information from the third party it is relying upon and does not need to request the customer to provide it with any verification documents. However, the subject person must have an agreement with the third party being relied upon for any such documents to be made available upon request and this arrangement must be tested from time to time to ensure that it actually functions as set out in the agreement. Moreover, the subject person remains responsible for the carrying out of a customer-based risk assessment, determining whether the customer is a PEP and conducting on-going monitoring.

In some instances, the regulatory regime applicable to the activities carried out by a subject person allows it to appoint agents as a means to extend their reach and carry on its business. Any business transacted by means of an agent is to be considered as business transacted by the subject person. As such any customer on-boarded or serviced by the agent has to undergo the same checks and controls as customers on-boarded and serviced by the subject person itself. It is therefore up to the subject person to ensure that its AML/CFT controls, policies, measures and procedures are applied to any such customer and the subject person may require that these be carried out by the agent.

The appointment of an agent is to be distinguished from outsourcing where the subject person engages a third party service provider to implement AML/CFT controls, policies, measures and procedures rather than carrying out the same itself. It is highly unlikely that the third party so engaged would limit its activities to those contracted with the subject person and it is usual for the third party service provider to have a number of contracts with different subject persons for the carrying out of the same service/s on their behalf.

Outsourcing within the context of AML/CFT is not at present allowed. However, the FIAU is currently evaluating this possibility and will be issuing a Consultation Document later on this year on outsourcing and the conditions that a subject person would have to adhere to be able to engage a service provider to implement its AML/CFT controls, policies, measures and procedures.

The common element in all these cases is that the subject person remains always responsible for ensuring it is adhering to its AML/CFT obligations.

[3] *For a better understanding of subject persons' obligations relative to the application of reliance, licensees are invited to consult article 25 to article 29 of the Directive. Section 3.6 of Part I of the current Implementing Procedures also provides a description of the current reliance procedure and how this should be applied. However, licensees are to note that this Chapter is to be revised by the FIAU as part of the transposition of the Directive into Maltese law and that substantial changes are to be made to those parts which stipulate which subject persons and third parties may be relied upon.*

4.1 Proposed Approach for the Remote Gaming Sector

Like any other subject person, licensees are able to exercise reliance to meet their CDD obligations as long as the conditions described above are met. It is important to note that the use of physical establishments as described in Section 3.1.2(i) does not amount to a reliance relationship as the physical establishment would be acting as an agent of the licensee and therefore is an extension of the same. In both instances, the physical establishment would allow a (prospective) customer to form a business relationship with, carry out an occasional transaction through or otherwise access the services or products offered by the licensees through the terminals present within the physical establishment.

In this regard and as set out in Section 3.1.2(i), it would be possible for the licensee to set up:

- Local physical establishments that would have to apply local AML/CFT requirements; and

- Physical establishments in jurisdictions outside Malta that would have to apply AML/CFT requirements applicable to the licensee but, to the extent that these physical establishments are themselves considered as equivalent to subject persons subject to supervision and equivalent AML/CFT requirements, the licensee would have the option to allow the physical establishments to apply their local AML/CFT requirements.

5. Reporting Suspicious Transactions[4]

5.1 Reporting Suspected or Known Instances of ML/FT

Subject persons are required to have internal and external procedures providing for the reporting of suspected or known instances of ML/FT. The internal reporting procedures must allow for subject person employees' to even report a suspected instance of ML/FT to the Money Laundering Reporting Officer ("MLRO") when their immediate superior is in disagreement with them. It will be then up to the MLRO to determine if the information available can be considered as sufficient for a Suspicious Transaction Report ("STR") to be made to the FIAU.

When the ML/FT suspicion is linked to a transaction still to be processed, it is important that the subject person refrains from carrying out the same, files a STR and delays the execution of the transaction for one (1) working day following the day on which the licensee files the STR. During this time the FIAU has to determine and communicate to the subject person whether it objects to the execution of the said transaction. Where refraining from carrying out the transaction is not possible or doing so would prejudice an analysis or investigation of the suspected instance of ML/FT, the subject person may decide to proceed with the transaction's execution. The impossibility to refrain from processing a transaction must arise from the nature of the transaction itself and the subject person must then submit a STR to the FIAU immediately afterwards.

5.2 Prohibition of Disclosure

The need not to prejudice an analysis or investigation into ML/FT is also at the basis of the non-disclosure obligations arising from filing a STR or receiving a request for information with the FIAU. Other than in exceptional cases which are provided for in Regulation 16(2) of the PMLFTR, a subject person cannot disclose any details or information in connection with a STR or a request for information made by the FIAU.

Safeguarding the integrity of an analysis or investigation is also why caution is advised when a subject person takes action to terminate a relationship or otherwise block a transaction following the filing of a STR. Drastic action should only be taken once the FIAU has been advised of the subject person's intentions as any unjustified action may alert the customer that he is being suspected of foul play. In such circumstances it would be more advisable to increase on-going monitoring and submit additional STRs to the FIAU on any other suspected instances of ML/FT.

5.3 Application to the Remote Gaming Sector

Licensees have already the obligation to report transactions they suspect to be linked to ML and the FIAU already receives a number of STRs every year from licensees. However, as a subject person the reporting obligations of a licensee are to be extended as follows:

[4] *For a better understanding of subject persons' reporting obligations, licensees are invited to consult article 33 to article 35 of the Directive. Chapter 6 of Part I of the current Implementing Procedures also provides a description of how the current reporting obligations are to be applied by subject person. Although no major changes are expected, licensees are to note that this Chapter is to be revised by the FIAU as part of the transposition of the Directive into Maltese law.*

i. The filing of a STR is not limited to transactions suspected of ML but extends to any suspicion that the licensee becomes aware of in the exercise of his business that a person is linked to ML/FT or that ML/FT is being committed or may be committed independently of whether any transactions have taken place or otherwise.

ii. A STR has to be filed not only in suspected instances of ML but also in situations where there is a suspicion of FT or that funds are the proceeds of crime.

iii. Reporting has to take place also when licensees have reasonable grounds to suspect that ML/FT may be taking place, this being a more objective ground for reporting. This implies that a further obligation to report arises where, on the basis of objective facts, the subject person ought to have suspected that ML/FT existed.

What kind of behaviour or transactions should alert licensees to a possible case of ML/FT and result in an internal report to the MLRO? There are red flags that may alert licensees but they are merely indicative and need not necessarily taken on their own point to ML/FT taking place. These red flags include:

- Customer does not cooperate in the carrying of CDD.
- Customer attempts to register more than one account with the same licensee.
- Customer deposits considerable amounts during a single session by means of multiple pre-paid cards.
- Customer deposit funds well in excess of what is required to sustain his usual betting patterns.
- Customer makes small wagers even though he has significant amounts deposits, followed by a request to withdraw well in excess of any winnings.
- Customer makes frequent deposits and withdrawal requests without any reasonable explanation.
- Noticeable changes in the gaming patters of a customer, such as when the customer carries out transactions that are significantly larger in volume when compared to the transactions he normally carries out.
- Customer enquires about the possibility of moving funds between accounts belonging to the same gaming group.
- Customer carries out transactions which seem to be disproportionate to his wealth, known income or financial situation.
- Customer seeks to transfer funds to the account of another customer or to a bank account held in the name of a third party.
- Customer displays suspicious behaviour in playing games that are considered as high risk.

In their considerations whether to submit a report to the FIAU, licensees are to bear in mind that:

i. AML legislation is intended to address and attack serious crime which usually either involves amounts that can be safely said to be other than minimal and/or show an intent to circumvent and abuse the safeguards in place to deter the use of the financial system for criminal purposes.

ii. Identity fraud and charge backs may give rise to ML but a licensee will only be subject to reporting obligations under AML/CFT legislation if they result in funds derived from these

activities being deposited with or held by the licensee. To the extent that the funds derived through these activities are deposited with another subject person, it will be the responsibility of that other subject person to file a report with its FIU.

The Authorities are aware that licensees often operate on a multi-jurisdictional basis and may therefore be considered as subject persons within a number of jurisdictions. Licensees may therefore encounter difficulties in determining to which authority they are to submit an STR. The Authorities can only outline what is their position in this regard, with licensees having to submit STRs to the FIAU whenever the suspicion of ML/FT arises in connection with activities conducted in term of a Maltese licence – it is after all this licence that renders licensees subject to AML/CFT requirements as they arise under Maltese law. Licensees should seek to acquaint themselves as much as possible with their AML/CFT obligations within the jurisdictions they operate as reporting obligations may be more stringent in some jurisdictions than others.

Licensees should be extremely careful on how they handle information related to STRs or to requests for information received from the FIAU, as well as how to deal with a customer that is the subject of a STR or a FIAU enquiry. The Authorities acknowledge that licensees may find themselves in a very uncomfortable position, especially in situations involving transactions that are still to be processed and which may therefore expose the licensee to complaints or even legal action. In this regard, the Authorities would like to point out that:

i. Pending transactions that are the subject of a STR cannot be processed for a determinate period of time following the submission of the STR. In part this is through the operation of the law and in part through the exercise of the FIAU's power to postpone transactions. If the period of postponement applicable by law (one working day following the day on which the licensee files the STR) expires and in the meantime the FIAU has not objected thereto or no court order has been issued, the licensee can proceed with processing the transaction if it deems the same not to pose any issue.

ii. Licensees should also remember that they are not in a position to disclose to the customer or to third parties that they filed a STR in his regard or that he is the subject of a request for information from the FIAU. And this independently of any other regulatory or contractual obligation that the licensee may be subject to. Licensees may however disclose as much to the MGA, where they are required to provide information by law.

iii. Any action that the licensee may want to take following the submission of a STR has to be properly considered to determine whether this may prejudice the analysis being conducted by the FIAU. Thus, licensees should be careful if they decide to block or close a customer's account, and should seek guidance from the FIAU's analysts prior to undertake any such action.

6. Funding of Terrorism

6.1 Funding of Terrorism

FT is the process of making funds or other assets available, directly or indirectly, to terrorist groups or individual terrorists to support them in their operations. This may take place through funds deriving from legitimate sources or from a combination of lawful and unlawful sources. Indeed, funding from legal sources is a key difference between terrorist organisations and traditional criminal organisations involved in money laundering operations.

Another difference is that while the money launderer moves or conceals criminal proceeds to obscure the link between the crime and the generated funds and avails himself of the profits of crime, the terrorist's ultimate aim is to obtain funds and resources to support terrorist operations.

Although it would seem logical that funding from legitimate sources would not need to be laundered, there is nevertheless often a need for terrorists to obscure or disguise links between the organisation or the individual terrorist and its or his legitimate funding sources. While ML is concerned with obscuring the source of the funds, FT is mostly concerned with obscuring the end recipient of the funds.

6.2 Funding of Terrorism and Gaming through Means of Distance Communications

In so far as gaming through means of distance communications are concerned, it has to be stressed that the risk of FT taking place presents itself predominantly at withdrawal stage. However, there may be indicators that a business relationship or an occasional transaction may expose the licensee to funding of terrorism risks even at inception stage. Examples include situations where (a) there is negative publicity implicating the customer with terrorism or organisations linked to terrorism; or (b) the customer has links to one or more jurisdictions or areas where terrorists are active or which are known to sympathise and support terrorists and terrorist organisations. The use of anonymous means of payment to fund an account in any such situation would further accentuate the risk of FT, especially when remitting funds withdrawn by the customer.

In the above situations it becomes imperative to carry out EDD even when the customer requests to withdraw the funds. Whatever the payment method used, it has to be ascertained that the institution to which the funds are remitted is situated in a reputable jurisdiction and has equivalent AML/CFT requirements as are applicable to the licensee. If the withdrawal is being made through a channel or a form that favours anonymity, the licensee has to the extent possible ascertain itself that it has established that the funds will eventually end up in the customer's hands.

APPENDIX 1

This appendix is intended to assist licensees in performing their assessment as to the level of risk posed by games, funding methods, and channels used. In the spirit of the risk-based approach advocated by the Directive, the rating provided below is indicative, and not necessarily mandatory. Notwithstanding this, any wide deviation therefrom would necessitate an explanation.

Risk mitigation measures adopted by a licensee to address the risk identified in specific items are also to be included in the risk assessment. The adoption of risk mitigating measures do not in themselves lower the risk identified, which is inherent to particular game, funding method or channel used, but are the means through which a licensee proposes to neutralize or manage the risk inherent in the said risk factors.

FUNDING METHODS

	Low	Low-Medium	Medium	Medium-High	High
Bank transfers (EEA or equivalent safeguards)	X				
Debit/credit cards issued by banks	X				
Debit/credit cards issued by other licensed financial institutions		X			
EEA-licensed payment service providers			X		
Non-EEA licensed PSP				X	
EEA-licensed PSP that can be funded with cash or quasi-cash				X	
Prepaid cards/vouchers					X
Cash					X

Examples of mitigating measures:

- Jurisdictions of operation, and the regulatory environment relating to payments;
- Methods used in processing payment of winnings to players (including procedures used when payments cannot be performed to the account of origin);
- Methods used in identifying origin of payments (ex: confirming that the account holder with the bank, card-issuer, or payments institution is the same as the gaming account holder);
- Strength of the operator's payments and anti-fraud team;
- Effectiveness of the operator's technological tools in place to monitor and detect suspicious activity.

GAME TYPES

	Low	Low-Medium	Medium	Medium-High	High
Fixed odds games without hedging (ex: slots, lotteries, bingo)	X				
Fixed odds games where hedging is possible (blackjack, baccarat, roulette)			X		
Sportsbetting			X		
P2P games (ex: poker, betting exchange)					X

Examples of mitigating measures:

- Strength of the operator's anti-fraud and anti-collusion department;
- Other safeguards against collusion (ex: external measures to impede a player choosing his or her opponent);
- Effectiveness of the operator's technological tools in place to monitor, prevent and detect fraud or collusion (ex: automated alerts on suspicious gameplay, chatroom/forum monitoring, dynamic and responsive risk management processes);
- Level of monitoring for sports integrity.

CHANNEL

	Low	Low-Medium	Medium	Medium-High	High
Remote & automated registration on an electronic platform without 3rd party intervention	X				
Facilitation of registration by a land-based intermediary				X	
Use of master account set-up					X

Examples of mitigating measures:

- Effectiveness of on-boarding procedures and associated safeguards;
- Effective control over land-based intermediary and access controls;
- Techniques used for monitoring of player activity;
- Regulatory environment and effective supervision carried out by local authorities.